EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Brian Tucker on 3/6/09.

AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1-8. (Cancelled)

9. (Currently Amended) In a client computing system, a method for participating in authentication with a server computing system, the method comprising:

an act of the client computing system receiving a first server request that includes at least a first indication of the authentication mechanisms deployed at the server computing system and a server nonce;

an act of the client computing system sending a first response to the server computing system and that includes a client public key, a client nonce and a selected set of the authentication mechanisms that were included in the first indication of the authentication mechanisms received from the server computing system and that are also deployed at the client computing system;

an act of identifying a tunnel key that can be used to encrypt content transferred between the client computing system and the server computing system, the tunnel key comprising a hash of a concatenation of a session key together with the server nonce and the client nonce;

Deleted: the

an act of receiving a second server request that includes encrypted authentication content, the encrypted authentication content being encrypted with the tunnel key and including a server challenge, a mutually deployed authentication method and a trust anchor;

an act of decrypting the encrypted authentication content with the tunnel key to reveal unencrypted authentication content, the unencrypted authentication content including the mutually deployed authentication mechanism the server challenge and the trust anchor; and

an act of sending a second response to the second server request, the second response including encrypted response data that is responsive to the unencrypted authentication content, including at least one of a client challenge, a hashed message authentication code that corresponds to the server challenge, or a client authentication signature, the encrypted response data being used for authenticating the client

computing system with the server computing system according to the mutually deployed authentication mechanism.

10. (Previously Presented) The method as recited in claim 9, wherein the first server request includes a previous packet ID corresponding to a previous session existing between the client and the server computing systems.

11. (Original) The method as recited in claim 9, wherein the authentication mechanisms deployed at the server computing system include one more authentication mechanisms selected from among MS-CHAP v2, Authentication with MD5, Authentication with Generic Token Card, Authentication with Kerberos, Authentication with X.509, and Authentication with WS-Security.

12. (Original) The method as recited in claim 9, wherein the authentication mechanisms deployed at the client computing system include one more authentication mechanisms selected from among MS-CHAP v2, Authentication with MD5, Authentication with Generic Token Card, Authentication with Kerberos, Authentication with X.509, and Authentication with WS-Security.

13. (Previously Presented) The method as recited in claim 9, wherein the first response includes a plurality of public keys.

14. (Cancelled).

15. (Previously Presented) The method as recited in claim 9, wherein the act of receiving the second server request comprises receiving encrypted authentication content corresponding to an authentication method selected from among: boot-strapping a client with an existing user-name and password, boot-strapping a client with an X.509 certificate, authenticating with an X.509 certificate, and boot-strapping a new client with a Kerberos token.

16. (Previously Presented) The method as recited in claim 15, wherein the second server request includes a previous packet ID.

17. (Previously Presented) The method as recited in claim 15, wherein the act of sending the second response includes sending encrypted responsive data for an authentication method selected from among: boot-strapping a client with an existing user-name and password, boot strapping a client with an X.509 certificate, authenticating with an X.509 certificate, and boot-strapping a new client with a Kerberos token.

18. (Previously Presented) The method as recite in claim 16, wherein the second response includes the previous packet ID.

19. (Currently Amended) In a server computing system, a method for participating in authentication with a client computing system, the method comprising:

an act of the server computing system sending a first request that includes at least a first indication of the authentication mechanisms deployed at the server computing system and a server nonce;

an act of the server computing system receiving a first client response to the first request and that includes a client public key, a client nonce and a selected set of the authentication mechanisms that were included in the first indication of the authentication mechanisms deployed by the server and that are also deployed at the client computing system;

an act of identifying a tunnel key that can be used to encrypt content transferred between the client computing system and the server computing system, the tunnel key comprising a hash of a concatenation of a session key together with the server nonce and the client nonce;

Deleted: the

an act of sending a second request that includes encrypted authentication content, the encrypted authentication content being encrypted with the tunnel key, the encrypted authentication content including a server challenge, a mutually deployed authentication mechanism and a trust anchor; and

an act of receiving a second client response, the second client response including encrypted response data that is responsive to the encrypted authentication content and that includes at least one of a client challenge, a hashed message authentication code corresponding to the server challenge, or a client authentication

signature, the encrypted response data being used for authenticating the client computing system with the server computing system according to the mutually deployed authentication mechanism.

20. (Previously Presented) The method as recited in claim 19, wherein the first request includes a previous packet ID corresponding to a previous session existing between the client and the server computing system.

21. (Original) The method as recited in claim 19, wherein the authentication mechanisms deployed at the server computing system include one more authentication mechanisms selected from among MS-CHAP v2, Authentication with MD5, Authentication with Generic Token Card, Authentication with Kerberos, Authentication with X.509, and Authentication with WS-Security.

22. (Original) The method as recited in claim 9, wherein the authentication mechanisms deployed at the client computing system include one more authentication mechanisms selected from among MS-CHAP v2, Authentication with MD5, Authentication with Generic Token Card, Authentication with Kerberos, Authentication with X.509, and Authentication with WS-Security.

23. (Previously Presented) The method as recited in claim 19, wherein the first client response includes a plurality of public keys.

24. (Cancelled).

25. (Previously Presented) The method as recited in claim 19, wherein the act of sending a second request comprises sending encrypted authentication content corresponding to an authentication method selected from among: boot-strapping a client with an existing user-name and password, boot-strapping a client with an X.509 certificate, authenticating with an X.509 certificate, and boot-strapping a new client with a Kerberos token.

26. (Previously Presented) The method as recited in claim 25, wherein the second request includes a previous packet ID.

27. (Previously Presented) The method as recited in claim 25, wherein the act of receiving a second client response includes receiving encrypted responsive data for an authentication method selected from among: boot-strapping a client with an existing user-name and password, boot strapping a client with an X.509 certificate, authenticating with an X.509 certificate, and boot-strapping a new client with a Kerberos token.

28. (Previously Presented) The method as recited in claim 27, wherein the second client response includes the previous packet ID.

29. (Previously Presented) The method recited in claim 9, wherein the first response also includes a plurality of security associations and wherein the second request includes one of the plurality of security associations selected from the plurality of security associations.

30. (Previously Presented) The method recited in claim 9, wherein the second response includes the client challenge.

31. (Previously Presented) The method recited in claim 9, wherein the second response includes the hashed message authentication code.

32. (Previously Presented) The method recited in claim 9, wherein the second response includes the client authentication signature.

Allowable Subject Matter

Claims 9 – 13, 15 – 23, and 25 – 32 are allowed.

The following is an examiner's statement of reasons for allowance:

The examiner notes that the claims essentially recite (e.g. see claims 9 and 19) a two part method for authentication, comprising first establishing a cryptographic tunnel and second practicing a mutually deployed authentication mechanism within the established cryptographic tunnel.

The examiner notes that the prior art similarly discloses a two part method of first establishing a cryptographic tunnel (e.g. a TLS link established by employing the a TLS tunnel key created according the known standard) between a server and client and then subsequently initiating a mutually deployed authentication mechanism (e.g. an challenge/response method such as MD5-CHAP of EAP) between the server and client (e.g. refer to Anderson, "Protected EAP Protocol (PEAP)"; Blunk, "PPP Extensible Authentication Protocol (EAP)").

Furthermore, the prior art method discloses the establishment of the cryptographic tunnel comprising the sending of messages between the client and server, the messages containing the recited "first indication of authentication mechanisms", *"a server nonce"*, *"a client public key"*, *"a client nonce"* and *"a selected set of the authentication mechanisms that … are also deployed at the client computing system"* (Anderson, pg. 7, par. 3 – pg. 8, par. 3).

However, the prior art does not appear to disclose, as found recited in combination, the claim limitations of the singular "first response" of a client comprising a set of authentication mechanisms selected from the received "first server request" wherein the "first server request" and the "first response" are characterized according to

method of "*an act of the client computing system receiving a first server request that includes at least a first indication of the authentication mechanisms deployed at the server computing system and a server nonce*" and "*an act of the client system sending a first response to the server computing system that includes a client public key, a client nonce and a selected set of the authentication mechanisms that were included in the first indication of the authentication mechanisms received from the server computing system and that are also deployed at the client computing system.*"

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFERY WILLIAMS whose telephone number is (571)272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

J. Williams
AU: 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437